

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA)	NO.: 17-cr-00630 (ER)
- v. -)	MEMORANDUM IN
)	SUPPORT OF MOTION TO
)	SUPPRESS
)	
MARK S. SCOTT,)	
)	
Defendant.)	ECF CASE
)	

The defendant, Mark S. Scott, by and through counsel and pursuant to the Fourth Amendment to the United States Constitution and Rules 12 and 41 of the Federal Rules of Criminal Procedure, and other cited authorities, respectfully moves this Honorable Court for the entry of an Order suppressing all evidence seized pursuant to a series of warrants executed on Mr. Scott's properties in August 2018.

Mr. Scott has been subjected to multiple constitutional violations, including:

1. The affidavits submitted in support of the search warrant applications fail to establish probable cause that Mark Scott engaged in criminal activity.
2. The affidavits fail to particularize the electronic devices to be seized and fail to tie their contents to criminal activity.
3. The warrants ultimately issued are unconstitutionally overbroad.
4. The warrants were executed in an unconstitutional manner because the seizures exceeded the scope of the warrants.
5. Electronic devices have been retained in a constitutionally unreasonable manner.

6. The government has knowingly seized privileged information without following established procedures.

I. Introduction

In September 2018, federal agents executed search warrants on properties owned by Mr. Scott, including homes in Florida and Massachusetts. The government seized multiple electronic devices as well as physical evidence. Supplemental search warrants followed.

The warrants were obtained based on the affidavits of Special Agent Kurt Hafer of the United States Attorney's Office for the Southern District of New York. The affidavits are not identical but are functionally equivalent. The warrants that were obtained based on affidavits from other agents incorporate the Hafer affidavit. Because of the multitude of warrants, the Florida warrant will be used as an example. (Affidavit of David Garvin in Support of Motion to Suppress: Exhibit A, Hafer Affidavit, Case 18-3283, Southern District of Florida).

The affidavit fails to establish probable cause to believe that Mark Scott engaged in criminal activity. The affidavit presents detail regarding the fraudulent nature of OneCoin and the activities of other individuals. But the affidavit fails to make the essential connection between Mr. Scott and criminal activity. There is nothing to show that Mr. Scott knew that funds that were to be invested were the proceeds of unlawful activity, an essential element of money laundering. It is not illegal to engage in transactions with proceeds of unlawful activity committed by others unless the defendant knows that the funds represent proceeds of unlawful

activity and the transactions are designed to promote the crime or hide the proceeds. That is significant here. Although the government implies that OneCoin is obviously fraudulent based on what it has unearthed, at the time of the transactions Mr. Scott did not have that information. OneCoin had not been declared unlawful by any government. Accordingly, the affidavit does not allege Mr. Scott knew about the problems with OneCoin.

Mr. Scott has standing because the material was seized from premises under his ownership or control.

II. The affidavit submitted in support of the search warrant application fails to establish probable cause that Mark Scott engaged in criminal activity.

The affidavit fails to establish probable cause that Mr. Scott was engaged in unlawful activity. The affidavit first notes that Mr. Scott was the subject of a sealed indictment. (Hafer Affidavit, Ex. A, page 3)(Hereafter Ex. A, ____). Next, the “overview” illustrates the blatant problem here: OneCoin is described as a pyramid scheme, but no facts are alleged indicating that Mark Scott either participated in the scheme or had knowledge that the funds involved were proceeds of unlawful activity. The overview claims that Mr. Scott met with one of the founders of OneCoin and then set up a series of hedge funds and ultimately received \$400 million of OneCoin proceeds. (Ex. A, 4). The affidavit states that Scott “lied” to banks about transactions, but the affidavit does not contain any allegation to satisfy the basic element of money laundering that the defendant knew that the funds were proceeds of unlawful activity.

The affidavit contains a background section on OneCoin. (Ex. A, 5-8). The affidavit describes the agent's conclusion that OneCoin is a fraudulent scheme. (Ex. A, 8-15). While this is one of the strongest sections of the affidavit, none of the allegations relate to Mr. Scott. The affidavit cites incriminating emails, but there is no allegation that Mr. Scott was copied on these messages or was aware of their contents.

The next section details OneCoin proceeds and again does not tie the information to Mr. Scott. (Ex. A, 15-17).

Turning to Mr. Scott's background, the affidavit sets out that Mr. Scott is an attorney and a member in good standing of the Florida Bar. (Ex. A, 17). The affidavit sets out Mr. Scott's businesses.

The section entitled "Scott's Use of Fenero Hedge Funds to Launder OneCoin Proceeds" states that Mr. Scott was introduced to an alleged coconspirator by email and that he was sent an encrypted telephone. (Ex. A, 19).

The affidavit says Mr. Scott formed businesses and opened bank accounts and received transfers of funds. (Ex. A, 19). The affidavit states that the funds consisted of money either directly or indirectly from OneCoin purchasers. (Ex. A, 20).

The affidavit then details purported "lies" to a fund administration firm and a bank. (Ex. A, 20-28). Essentially the affidavit claims that Mr. Scott misrepresented the source of the funds.

The affidavit then details financial transfers and purchases made by Mr. Scott. (Ex. A, 28-33). Again, there is no allegation that Mr. Scott participated in or, more importantly, knew about the alleged underlying fraudulent conduct.

From these allegations, the affidavit argues that there is probable cause for searching the premises and seizing electronically stored information. (Ex. A, 33-36).

Whether the search involves the search for physical evidence or for computerized records, the fundamental requirement of the Fourth Amendment is that the affidavit establish probable cause:

The Fourth Amendment's Warrants Clause provides that "no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." The clause was intended as a bulwark against "the 'general warrant' abhorred by the colonists" and protects against "a general, exploratory rummaging in a person's belongings." *Coolidge v. New Hampshire*, 403 U.S. 443, 467, 91 S. Ct. 2022, 29 L. Ed. 2d 564 (1971). Its overarching purpose is to ensure that "those searches deemed necessary should be as limited as possible." *Id.*

To achieve its goal, the Warrants Clause requires particularity and forbids overbreadth. "Particularity is the requirement that the warrant must clearly state what is sought. Breadth deals with the requirement that the scope of the warrant be limited to the probable cause on which the warrant is based." *United States v. Hill*, 459 F.3d 966, 973 (9th Cir. 2006). ...[A] warrant can violate the clause "either by seeking specific material as to which no probable cause exists, or by giving so vague a description of the material sought as to impose no meaningful boundaries." *Id.* at 359.

United States v. Cioffi, 668 F. Supp. 2d 385, 390 (E.D.N.Y. 2009). *United States v. Wey*, 256 F. Supp. 3d 355, 379 (S.D.N.Y. 2017). The *Wey* case includes a comprehensive discussion of Fourth Amendment standards as applied to a search for primarily electronic records, and Mr. Scott adopts the standards set out in *Wey*

regarding probable cause, particularity, overbreadth, timing and execution of the warrant.

This affidavit wholly fails to establish probable cause that Mr. Scott engaged in or conspired to commit the cited money laundering offenses. The argument here is very simple and is plain from the face of the cited statutes: the money laundering offenses cited at page 3 of the affidavit require a showing that the defendant knew that the funds were proceeds of unlawful activity. 18 U.S.C. § 1956(a)(1), 1956(a)(2)(B)(i). No such showing is made or attempted other than to insinuate that Mr. Scott's clients were secretive by using a secure phone for international calls and that Mr. Scott did not tell third parties who the investors were.

Bank fraud under 18 U.S.C. § 1344 is also cited in the affidavit, but no real effort is made to establish bank fraud. Bank fraud requires a scheme to defraud the financial institution or to obtain money under the control of the financial institution. 18 U.S.C. § 1344. The purported misrepresentation to a bank is cited as an attempt to disguise the proceeds rather than to obtain funds from the bank. (See Ex. A, p. 26, par. 22).

Even if the affidavit established probable cause that the operators of OneCoin in Europe committed fraud, the affidavit fails to establish that evidence of those offenses would be located in Mr. Scott's residences.

III. The affidavits fail to particularize the electronic devices to be seized and fail to tie their contents to criminal activity.

The warrants authorize the seizure of computers and electronic devices. In fact, the warrants that were prepared using the Attachment A prepared by the

government authorized the seizure of “any computer devices and storage media that may contain any electronically stored information.” (Affidavit of David Garvin in Support of Motion to Suppress: Exhibit B, Search and Seizure Warrant). Thus, the government requested and received authority to seize any and all electronic devices regardless of whether there was any showing of a nexus to criminal activity. Here, the warrants violate the particularity clause of the Fourth Amendment and transform this into a general warrant. *See Maryland v. Garrison*, 480 U.S. 79, 85 (1987) (“By limiting the authorization to search to the specific areas and things for which there is probable cause to search, the requirement ensures that the search will be carefully tailored to its justifications . . .”). The less precise the description of the place to be searched or things to be seized, the less likely there is probable cause to seize the enumerated items. For example, if a description is broader than can be justified by the probable cause upon which the warrant is based, the description could be defective. *See VonderAhe v. Howland*, 508 F.2d 364 (9th Cir. 1974) (finding warrant invalid where government knew what financial records it sought but requested all records relating to the defendant’s finances). Generality is permitted when greater specificity is impossible or when the scheme investigated is particularly complex. *See Andreson*, 427 U.S. at 480 n.10 (complex nature of real estate scheme under investigation must allow for some generality of description). And, although there are instances when an affidavit can establish probable cause that a business is so “permeated with fraud” that virtually all records can be seized, the affidavit made no attempt to do so in this case. Furthermore, the “permeated

with fraud" showing must be made in the affidavit and not by relying on what was actually seized. *See United States v. Ford*, 184 F.3d 566, 576 (6th Cir. 1999) (conviction reversed because search warrant authorized broader search than reasonable --"Even if one business carried on at a site is permeated with fraud, if other businesses run at the same site are separable and are not shown to be related to the suspected crime, a warrant permitting seizure of all documents at the site is not justified."); *United States v. Kow*, 58 F.3d 423 (9th Cir. 1995) (conviction reversed where warrant failed to identify business records with particularity, and good faith exception did not apply); *United States v. McGrew*, 122 F.3d 847 (9th Cir. 1997) (conviction reversed because search warrant affidavit lacked particularity); *In re Grand Jury Investigation*, 130 F.3d 853 (9th Cir. 1997) (conviction reversed because search warrant was overbroad).

The Fourth Amendment commands that no warrants shall issue except those "particularly describing the place to be searched, and the . . . things to be seized." U.S. Const. amend. IV. The purpose of the particularity requirement is to make "general searches . . . impossible and prevent[] the seizure of one thing under a warrant describing another. As to what is to be taken, nothing is left to the discretion of the officer executing the warrant." *Marron v. United States*, 275 U.S. 192 (1927). *See also Andreson v. Maryland*, 427 U.S. 463, 480 (1976); *United States v. Blakenev*, 942 F.2d 1001 (6th Cir. 1991) ("A general order to explore and rummage through a person's belongings is not permitted."). Warrants that contain

broad descriptions constitute general exploratory warrants which the Framers intended to prohibit.

Here, there was no showing that any of the devices that were ultimately seized was used to further unlawful activity or contained evidence. In fact, several devices were seized that had not been used since before any of the OneCoin related conduct mentioned in the affidavit. The government seized and has provided an image of at least fifteen devices, many of which contain no relevant evidence – including devices only used by Mr. Scott's wife.

This is a very different situation than the process that was affirmed by the Second Circuit in *United States v. Ulbricht*, 858 F.3d 71, 103-04 (2d Cir. 2017). In that case the Second Circuit noted that the digital devices were involved in a “symbiotic” relationship to Ulbricht’s operation of the Silk Road site on the dark web:

Finally, we note that the crimes charged in this case were somewhat unusual. This case does not involve a more typical situation in which officers searched for evidence of a physician’s illegal distribution of pain medications, to use the NACDL’s example, which may have electronically-stored data associated with the alleged crimes on a hard drive that largely contains non-criminal information. Here the crimes under investigation were committed largely [*104] through computers that there was probable cause to believe included the laptop at issue, and the search warrant application gave ample basis for the issuing magistrate judge to conclude that evidence related to Silk Road and Ulbricht’s use of the DPR username likely permeated Ulbricht’s computer. Thus, given the nature of Ulbricht’s crimes and their symbiotic connection to his digital devices, we decline to rethink the well-settled Fourth Amendment principles that the Laptop Warrant may implicate. A future case may require this Court to articulate special limitations on digital [**54] searches to effectuate the

Fourth Amendment's particularity or reasonableness requirements. Such a case is not before us.

United States v. Ulbricht, 858 F.3d 71, 103-04 (2d Cir. 2017).

In *Ulbricht*, the affidavit showed sufficient use of the digital devices to commit crimes that the devices were sufficiently particularized. That is not so here, where there is nothing special about the devices other than that they store data, in the same way that all devices do.

The court also made it clear that “the warrant must specify the items to be seized by their relation to designated crimes.” *United States v. Ulbricht*, 858 F.3d 71, 99 (2d Cir. 2017)(quoting *United States v. Galpin*, 720 F.3d 436, 445 (2d Cir. 2013)(internal quotations omitted)). That nexus is missing here. The affidavit not only does not specify which electronic devices should be seized; it also fails to show their relationship to the designated offenses. *See also United States v. Rosa*, 626 F.3d 56, 60-61 (2d Cir. 2010)(warrant for computerized records failed to describe with particularity the evidence to be seized and “to link that evidence to the criminal activity supported by probable cause.”); *United States v. Buck*, 813 F.2d 588, 592 (2d Cir. 1987).

IV. The warrants ultimately issued are unconstitutionally overbroad.

For the same reasons, the warrants are functionally general warrants because they allowed the officers discretion to seize essentially every document in Mr. Scott’s possession. In addition to the fact that the warrants allow the seizure of all computers and electronic devices, the warrant essentially allowed the officers complete discretion to seize any records as long as they found them to be evidence of

the listed offenses. There was no particularization other than a paragraph that listed certain businesses and individuals but specifically noted that the seizure was “not limited to” those items. (Ex. B. p. 3, II Items to Be Seized).

Further, some of the supplemental warrants provide no particularization at all but merely authorized the seizure of evidence of certain offenses:

ITEMS TO BE SEIZED

The items to be seized from the Subject Premises include the following:

All evidence, fruits, and instrumentalities of Title 18, United States Code, §§ 1956(a)(1)(B)(i), 1956(a)(2)(B)(i), 1956(h), and 1344 (money laundering, conspiracy to commit money laundering, and bank fraud), related to the OneCoin business and derived funds (the “Subject Offenses”), including but not limited to: (i) documents and communications relating to the administration of the OneCoin business, and the transfer and/or laundering of criminal proceeds; (ii) currency or financial instruments; (iii) bank documents including teller receipts or withdrawal tickets; and (iv) bank envelopes or cash pouches.

(Exhibit C: Search and Seizure Warrant, In the matter of the Search of Safe Deposit Box, No. 18-mj-5112-JGD (D.Mass. 9/25/2018). Thus, the warrant is a clearly prohibited “all evidence” warrant, leaving the execution to the sole discretion of the executing agents.

The warrants here lack sufficient particularization as was the case in *Wey*:

In sum, the Warrants authorize the seizure of sweeping categories of materials, regardless of their potential connection (or lack thereof) to any suspected criminal activities and limited only by the requirement that they relate in some generalized way to the owner/occupant of the very premises subject to search. The conferral of such unfettered discretion on the executing officers, particularly in light of the Warrants’ independent failure to identify any crime under investigation, is inconsistent with the Fourth Amendment’s particularity requirement.

United States v. Wey, 256 F. Supp. 3d 355, 387 (S.D.N.Y. 2017).

Additionally, the warrant's authorization for the seizure of electronic information is overbroad because it contains no date restriction. (Ex. B, 3-4).

United States v. Wey, 256 F. Supp. 3d 355, 387 (S.D.N.Y. 2017).

V. The warrants were executed in an unconstitutional manner because the seizures exceeded the scope of the warrants.

Executing agents grossly exceeded the scope of the already overbroad warrants.

Executing officers are not restricted to seizing *only* named items, but any additional items seized must meet the following test: (1) that the article seized be "of incriminating character and (2) that it be immediately apparent" to the police that this is so. *See Coolidge v. New Hampshire*, 403 U.S. 443 (1971). *See also Andreson v. Maryland*, 427 U.S. 463 (1976) (providing that a court must consider what the executing officers knew about the nature of the crime, its elements, and possible means of proving those elements when determining what unnamed items may be seized as evidence of the crime for which the search warrant issued).

Rather, the government seized documents and computer files unrelated to the alleged wrongdoing and unmentioned in the warrant because it was easier to seize everything than to seize only those documents and computer files for which they had probable cause. This was unreasonable.

Just a few examples of items seized without regard to the warrant are:

- Wedding photographs
- Fertility treatment documents

- Medical Records of family members
- Mr. Scott's wife's phone and computer
- Jewelry that was possessed long before the questioned conduct
- Mr. Scott's mother's will

Where, as here, the executing agents grossly exceeded the scope of the warrant, the remedy is suppression of all evidence seized pursuant to the warrant.

United States v. Medlin, 842 F.2d 1194, 1199 (10th Cir. 1998); *United States v. Foster*, 100 F.3d 846, 851 (10th Cir. 1996). Convictions are reversed when the scope of the warrant is exceeded. *See e.g., Marks v. Clark*, 102 F.3d 1012 (9th Cir. 1997) (conviction reversed where warrant to search two residences did not authorize the officers to search all persons present); *United States v. Schroeder*, 129 F.3d 439 (8th Cir. 1997) (conviction reversed because warrant did not authorize search of adjoining property); *see also Leveto v. Lapina*, 258 F.3d 156 (3rd Cir. 2001) (holding that warrant for home did not justify pat-down of owner).

VI. Electronic devices have been retained in a constitutionally unreasonable manner.

The government has kept the electronic devices and documents, including irrelevant documents, for eight months. The warrants detailed a methodology for examining seized electronic data. That methodology has not been followed. The affidavit sets out methods for review and says that if the Government determines that electronic devices are no longer necessary to retrieve and preserve the data and the devices themselves are not subject to seizure pursuant to Federal Rule of Criminal Procedure 41(c), the Government would return the items. None have been returned. Defense counsel have received a copy of a forensic image of the devices

that takes special software to review. Mr. Scott has been deprived of this property. The property should be returned with the government ordered not to retain a copy. *See United States v. Ganias*, 824 F.3d 199, 217, 2016 U.S. App. LEXIS 9706, (2d Cir. Conn. May 27, 2016)(en banc)(declining to determine whether there was a constitutional violation and relying on the good faith exception, but noted in dicta, “we do not mean to thereby minimize or ignore the privacy concerns implicated when a hard drive or forensic mirror is retained, even pursuant to a warrant. The seizure of a computer hard drive, and its subsequent retention by the government, can give the government possession of a vast trove of personal information about the person to whom the drive belongs, much of which may be entirely irrelevant to the criminal investigation that led to the seizure.”). That is exactly what has occurred here. The government has seized a vast amount of personal information that is unrelated to any showing of probable cause.

VII. The government has knowingly seized privileged information without following established procedures.

Mr. Scott is a practicing lawyer. The government was aware of Mr. Scott’s profession at the time of the seizure. Nevertheless, the government seized the entirety of Mr. Scott’s electronic devices. Although the government purports to have a taint team in place, upon information and belief, Mr. Scott asserts that the government has reviewed privileged information in an unreasonable manner. The warrant itself dictated that “review of the items described in this attachment shall be conducted pursuant to established procedures designed to collect evidence in a manner reasonably designed to protect any attorney-client or other applicable

privilege.” (Ex. B, 2). However, there were no “established procedures” mentioned, nor put in place. Some of the material seized is both privileged and outside the scope of any alleged criminal conduct. Undersigned counsel believe that the government did nothing to engage taint team until months after the seizure.

VIII. Conclusion

For the foregoing reasons, Mr. Scott respectfully requests this Honorable Court to order the suppression and return of the items seized pursuant to the various search warrants executed in this case.

Dated: May 14, 2019

Respectfully submitted,

/s/ David M. Garvin
David M. Garvin
Counsel for Defendant, Mark S. Scott
DAVID M. GARVIN, P.A.
200 South Biscayne Boulevard
Suite 3150
Miami, Florida 33131
Tel: (305) 371-8101
Fax: (305) 371-8848
Email: ontrial2@gmail.com

CERTIFICATE OF SERVICE

I hereby certify that on May 14, 2019, I electronically filed Defendant's Memorandum in Support of Motion to Suppress with the Clerk of the District Court using its CM/ECF system, which would then electronically notify the parties in this case:

Christopher Joseph DiMase, AUSA

Julieta Veronica Lozano, AUSA

Nicholas Folly, AUSA

James Nobles, Esq.

/s/ David M. Garvin

David M. Garvin, Esq.

Counsel for Defendant, Mark S. Scott

DAVID M. GARVIN, P.A.

200 South Biscayne Boulevard Suite 3150

Miami, Florida 33131

Tel: (305) 371-8101

Fax: (305) 371-8848

Email: ontrial2@gmail.com